Contratos informáticos en Argentina

Continuidad operativa, depósito de código fuente y servicios de infraestructura

IT Contracting in Argentina: Business continuity, source code escrow and infrastructure provision

Mariano Enrique Torres Ponce

Abogado y Especialista en Derecho Informático

ORCID: 0009-0009-6284-3867

Agosto de 2019

Edición navegable y accesible. El contenido se mantiene sin modificaciones.

Resumen

El trabajo analiza la contratación informática en el derecho argentino desde una perspectiva orientada a la protección de la continuidad operativa del usuario. Se observa que el software y los servicios tecnológicos se han integrado a la estructura productiva de las empresas, generando una dependencia técnica que exige adaptar la técnica contractual para evitar que una falla o interrupción comprometa el normal desarrollo del negocio. El artículo examina el deber de información en la etapa precontractual, el alcance del derecho de uso del software y las obligaciones de mantenimiento asociadas, así como las herramientas preventivas que buscan preservar la funcionalidad de los sistemas frente a contingencias. Se estudia la responsabilidad del proveedor en materia de seguridad y custodia de datos, y se destacan mecanismos de resiliencia tecnológica como el depósito del código fuente y los acuerdos de nivel de servicio. El enfoque se apoya en principios generales del Código Civil y Comercial de la Nación, y en doctrina nacional especializada en contratos informáticos. Se concluye que un contrato correctamente diseñado permite compatibilizar la protección del creador con la estabilidad económica del usuario, garantizando que la innovación tecnológica se consolide como fuente de competitividad y no de vulnerabilidad.

Palabras clave

contratos informáticos, derecho privado argentino, continuidad operativa, dependencia tecnológica, depósito de código fuente, servicios informáticos en línea, seguridad de la información, responsabilidad contractual, protección de datos, resiliencia tecnológica

Abstract

This article analyzes IT contracting under Argentine private law, focusing on the protection of business continuity for users who rely on technological systems as essential components of their operations. Software and digital services create a technical dependency that requires contractual safeguards capable of preventing commercial disruption in case of failure or interruption. The study examines the duty of disclosure during pre-contractual negotiations, the legal scope of software usage rights, and the obligations of maintenance and support that ensure ongoing functionality. It also addresses risk-mitigation tools such as source code escrow, service level agreements, and data security requirements, which aim to preserve operational resilience. The analysis relies on the general principles of the Argentine Civil and Commercial Code and on local legal scholarship regarding IT contracts. The conclusion highlights that a well-structured contract can harmonize the provider's intellectual property rights with the user's economic stability, ensuring that technological innovation remains a source of competitiveness rather than vulnerability.

Keywords

IT contracts, Argentine private law, business continuity, technological dependency, source code escrow, online service provision, information security, contractual liability, data protection, technological resilience

Índice

Resumen **2**
Palabras clave 2

Abstract **3**
Keywords 3

1 Introducción **5**

2 Contratación informática y dependencia tecnológica en el derecho argentino **7**

3 Etapa precontractual y deber de información en proyectos tecnológicos **10**

4 Software y derechos de uso. Alcance funcional y protección del cliente **12**

5 Depósito del código fuente para asegurar la continuidad operativa **14**

6 Hosting y provisión de servicios informáticos en línea **16**

7 Seguridad, datos y responsabilidad en entornos digitales **18**

8 Criterios contractuales para la resiliencia tecnológica **20**

9 Conclusiones **22**

Bibliografía **24**

Capítulo 1

Introducción

La expansión sostenida de la tecnología en las actividades económicas modificó de manera profunda la estructura de las relaciones jurídicas privadas. Las empresas de todos los sectores apoyan su funcionamiento en sistemas informáticos que administran procesos internos, almacenan datos estratégicos y permiten interactuar con terceros de manera ágil y segura. La dependencia de estas herramientas dejó de ser un fenómeno incidental para convertirse en la base que sostiene la continuidad operativa de los negocios. El contrato pasó a ocupar un lugar central en esta realidad, ya que es el instrumento mediante el cual se asignan riesgos y se preservan intereses económicos que se verían severamente afectados si la infraestructura tecnológica fallara o quedara momentáneamente inactiva. La contratación informática en Argentina se consolidó así como un espacio relevante dentro del derecho privado, donde la función práctica del acuerdo adquiere una intensidad mayor respecto de los contratos tradicionales, especialmente cuando la prestación consiste en mantener en funcionamiento una solución técnica necesaria para que una empresa pueda operar sin interrupciones (Altmark, 1987).

El contenido operativo del contrato cumple un papel decisivo porque define la estabilidad de la prestación como factor económico indispensable. El valor del software no reside en la materialidad del soporte ni en la titularidad abstracta de derechos, sino en la posibilidad concreta de usar la herramienta para el desarrollo regular del negocio. Cuando el sistema informático se vuelve crítico y no existen alternativas inmediatas de reemplazo, surge una posición de dependencia tecnológica que genera riesgos jurídicos específicos. El incumplimiento del proveedor no se agota en frustrar la expectativa del cliente, sino que puede paralizar su actividad o exponerlo frente a terceros. Por esa razón la buena fe contractual adquiere un contenido práctico que obliga a prever contingencias y mecanismos de protección orientados a sostener la continuidad del servicio comprometido (Cibils, 2015).

El ordenamiento jurídico argentino ofrece un marco suficiente para regular estas

relaciones a través del Código Civil y Comercial de la Nación, que garantiza la libertad contractual y refuerza el deber de cooperación entre las partes. Sin embargo, la ausencia de una regulación sectorial obliga al contrato a cumplir una función de precisión técnica más rigurosa. Cada cláusula debe describir responsabilidades y medidas de actuación que permitan mantener la utilidad del sistema en el tiempo, porque la finalidad del usuario no consiste en adquirir un producto aislado, sino en asegurarse el acceso permanente a una herramienta funcional que sostiene su desempeño en el mercado. La interpretación debe enfocarse en esa finalidad económica, evitando soluciones que desconozcan el rol estructural que la tecnología cumple en la organización del cliente (Lorenzetti, 2015).

La dinámica propia del desarrollo informático incluye elementos que pueden alterar el equilibrio contractual, como la evolución de los sistemas, la necesidad de actualizaciones y la posibilidad de que el proveedor modifique su estrategia comercial o desaparezca del sector. Frente a ese escenario cambiante se vuelve indispensable la incorporación de garantías preventivas. El derecho no solo protege a través de remedios posteriores al incumplimiento, sino también mediante herramientas diseñadas para evitar que el usuario quede sin alternativas de funcionamiento si se presenta una contingencia técnica o empresarial significativa. De allí surge la relevancia de instituciones como el depósito del código fuente, los niveles mínimos de disponibilidad del servicio y los compromisos de mantenimiento continuo, cuyo desarrollo contractual apunta a reforzar la resiliencia del negocio frente al riesgo tecnológico (Martínez Barbieri, 2011).

El contrato informático debe funcionar entonces como una estructura jurídica capaz de absorber la complejidad técnica que lo integra. No alcanza con un acuerdo formalmente válido si este no incluye los elementos indispensables para asegurar la continuidad operativa del usuario. La protección jurídica en este campo se mide en términos de estabilidad y seguridad de la prestación, por lo que la técnica contractual debe asumir un rol activo y anticipatorio. Esta perspectiva orienta el análisis que se desarrollará en los capítulos siguientes, en los cuales se abordarán los aspectos esenciales de la contratación vinculada al software y a la infraestructura digital, identificando los instrumentos que permiten resguardar al usuario frente a la dependencia tecnológica que él mismo asume al adoptar soluciones informáticas como pilar de su actividad.

Capítulo 2

Contratación informática y dependencia tecnológica en el derecho argentino

La creciente incorporación de sistemas informáticos en los procesos de producción y gestión de las empresas argentinas instaló un nuevo modo de entender la contratación privada. Los proveedores de soluciones tecnológicas no solo entregan un bien inmaterial o habilitan un acceso, sino que asumen un papel directo en el sostenimiento cotidiano de la actividad económica del usuario. La disponibilidad del sistema se convierte en un factor determinante para el cumplimiento de obligaciones comerciales, financieras y operativas del cliente. La contratación informática se transforma en una herramienta que organiza jurídicamente esta realidad y define qué ocurre cuando el componente tecnológico del negocio enfrenta fallas o interrupciones que pueden comprometer su normal desarrollo. La doctrina local advirtió que esta dependencia transforma el contrato en un instrumento de protección económica de alta sensibilidad, donde las consecuencias del incumplimiento se magnifican respecto de los contratos tradicionales vinculados a bienes materiales (Cibils, 2015). Esta configuración refuerza la idea de que el servicio tecnológico deja de ser complementario para convertirse en una pieza central de la infraestructura empresarial, cuya indisponibilidad puede afectar gravemente la posición competitiva del usuario y su capacidad de cumplir con obligaciones frente a terceros.

En este tipo de relaciones el usuario habitualmente no tiene control sobre la estructura técnica de la prestación y debe confiar en el proveedor para que la solución se mantenga estable en el tiempo. No se trata de un contrato estático que se agota con la entrega del producto, sino de una vinculación de tracto sucesivo en la cual la utilidad del servicio se renueva cada día que el sistema permite la continuidad del negocio. Esta característica implica una distribución de riesgos diferente, porque la afectación del

servicio puede paralizar la operatoria del cliente o afectar su reputación en el mercado. La buena fe adquiere aquí un contenido operativo, no solo declarativo, que exige al proveedor un comportamiento diligente acorde al rol técnico que desempeña en la estructura empresarial del usuario (Lorenzetti, 2015).

La dependencia tecnológica genera también un plano de asimetría informativa marcado por la posición del proveedor como experto en la configuración y mantenimiento del sistema. La especificidad del objeto informático y la brecha de conocimientos entre las partes exigen un mayor rigor en la determinación contractual de obligaciones, ya que el usuario deposita su capacidad operativa en la intervención técnica del prestador (Molina Quiroga, 2001). Este conocimiento diferencial permite anticipar dificultades que el cliente no está en condiciones de advertir por sí mismo, lo que refuerza la necesidad de incorporar soluciones que equilibren la relación. La protección jurídica se materializa cuando los riesgos previsibles se traducen en cláusulas claras que definan la responsabilidad del proveedor y garanticen la continuidad del funcionamiento del sistema.

La responsabilidad derivada de la interrupción del servicio también debe evaluarse en función del rol decisivo que cumple el proveedor en el negocio del usuario. La diligencia del prestador en contratos informáticos debe interpretarse con un estándar técnico elevado, ya que la falta de mantenimiento, de actualización o de soporte adecuado puede constituir un incumplimiento grave que afecte directamente el desempeño económico del cliente (Molina Quiroga, 2013). La seguridad del negocio del usuario se vuelve el parámetro central para evaluar el equilibrio contractual y la prestación se interpreta a partir de esa finalidad práctica predominante (Pérez Luño, 2016).

El derecho argentino dispone de principios suficientes para albergar estas modalidades contractuales sin necesidad de crear una categoría normativa autónoma. El Código Civil y Comercial de la Nación reconoce el valor de la negociación libre y la fuerza obligatoria del contrato, y brinda criterios hermenéuticos que permiten adecuar el contenido de la prestación a su función económica concreta. La técnica jurídica aplicada a los contratos informáticos debe profundizar en la descripción de los elementos funcionales del sistema, establecer obligaciones de mantenimiento y prever mecanismos de actuación que protejan al usuario frente a la posible indisponibilidad de la solución tecnológica adoptada. El contrato deja de ser una simple distribución formal de obligaciones y pasa a constituirse en la principal herramienta para sostener la resiliencia operativa de quien depende del servicio para existir económicamente.

En síntesis, la contratación informática en Argentina se sitúa en un espacio donde se entrecruzan la libertad contractual, el interés económico del usuario y la dimensión técnica de la prestación. La clave se encuentra en alcanzar un equilibrio real entre derechos intelectuales del proveedor y continuidad operativa del cliente, de modo que la

dependencia tecnológica no derive en un riesgo excesivo para quien confía su negocio a una infraestructura que no controla. Este enfoque permite articular la innovación tecnológica con una tutela jurídica suficiente, evitando que el progreso digital se traduzca en vulnerabilidad contractual.

Capítulo 3

Etapa precontractual y deber de información en proyectos tecnológicos

La etapa precontractual en los contratos informáticos adquiere una relevancia jurídica singular, ya que en ese momento se determina la adecuación del sistema a las necesidades reales del usuario. La complejidad técnica de muchos desarrollos y la falta de conocimientos especializados del cliente generan una asimetría que obliga al proveedor a brindar información suficiente y precisa sobre las características, limitaciones y condiciones de uso de la solución que ofrece. La lealtad negocial exige que quien posee el conocimiento técnico permita que la contraparte contrate sobre la base de expectativas realistas y correctamente fundadas. La doctrina argentina, desde una perspectiva general, ha entendido que la buena fe debe regir las tratativas preliminares y que su violación puede generar responsabilidad por los daños que deriven de una confianza defraudada (Altmark, 1987).

En este contexto, la fase de relevamiento y análisis funcional del proyecto no es solo un procedimiento técnico, sino también un elemento determinante de la futura asignación de riesgos. Lo que se documenta en esta instancia condiciona el objeto del contrato, ya que define el alcance del servicio que el proveedor se comprometerá a prestar y los resultados que el usuario espera obtener del sistema informático. Si el proveedor omite advertir aspectos esenciales que pueden afectar el funcionamiento o la integración con otros sistemas utilizados por el cliente, se produce un déficit informativo incompatible con el rol profesional que se asume al ofrecer una solución tecnológica para la operatoria de una empresa.

La responsabilidad precontractual se manifiesta cuando la conducta del proveedor induce al usuario a celebrar un contrato que no satisface los fines prácticos que motivaron la contratación y esa insatisfacción responde a circunstancias que el profesional conocía o razonablemente debía conocer. La doctrina coincide en que la reparación de los daños en esta instancia no se limita a los gastos realizados durante las tratativas, si-

no que puede extenderse a la pérdida de oportunidad o a las consecuencias negativas que genera haber confiado en una promesa técnica infundada. La función preventiva de la buena fe se acentúa frente a la naturaleza técnica de la prestación, ya que el usuario deposita su confianza en una experiencia ajena que resulta indispensable para la toma de decisiones informadas (Cibils, 2015).

El ordenamiento argentino aborda esta problemática desde principios generales sin necesidad de regulación específica. La teoría de la responsabilidad por ruptura injustificada de negociaciones y la tutela de la confianza legítima funcionan adecuadamente para proteger al usuario frente a maniobras que alteran el equilibrio de la relación antes de que se perfeccione el contrato. En la contratación informática, estas soluciones tienen especial eficacia porque la posición debilitada del cliente se vincula directamente con su desconocimiento de los riesgos tecnológicos involucrados. La doctrina ha destacado que la transparencia en esta fase inicial no solo contribuye a una asignación de riesgos más equitativa, sino que reduce la probabilidad de conflictos futuros y fortalece la utilidad práctica del contrato como instrumento de estabilidad operativa (Lorenzetti, 2015).

En síntesis, la etapa precontractual en los contratos informáticos se erige como un momento estructural que condiciona la eficacia económica y jurídica de la relación. La protección del usuario no se agota en sancionar incumplimientos posteriores, sino que comienza con la exigencia de una conducta informada, diligente y orientada a detectar con anticipación las necesidades reales del negocio que se pretende sostener con tecnología. Un proyecto bien definido desde el inicio constituye la primera barrera de defensa frente al riesgo tecnológico y evita que la dependencia técnica del usuario se transforme en vulnerabilidad jurídica.

Capítulo 4

Software y derechos de uso. Alcance funcional y protección del cliente

El software se presenta como un bien inmaterial protegido por el derecho de autor y destinado a ser explotado mediante licencias de uso que definen con precisión el modo en que el usuario puede interactuar con la herramienta. La contratación informática en Argentina se estructura principalmente sobre este modelo, donde la titularidad sobre el programa permanece en cabeza del desarrollador y el cliente accede únicamente a una facultad de utilización condicionada por lo pactado. Esta configuración reconoce la inversión intelectual del proveedor, pero al mismo tiempo genera un escenario de dependencia operativa del usuario, que no posee los medios técnicos para sostener la funcionalidad del sistema sin la colaboración del titular del software (Andreucci, 2016).

El derecho de uso, por lo tanto, no garantiza por sí solo que el programa mantenga su eficacia a lo largo de toda la vigencia del contrato. La utilidad del software se mantiene únicamente si continúa siendo compatible con la infraestructura del cliente, se actualiza frente a cambios tecnológicos y se corrigen los errores que surgen en el funcionamiento real. Cuando el sistema forma parte de la estructura esencial del negocio del usuario, cualquier interrupción puede traducirse en pérdidas económicas concretas y afectar incluso la relación con terceros. La interpretación contractual debe orientarse hacia esta finalidad práctica predominante, ya que la prestación no consiste en la entrega de un producto terminado, sino en asegurar que su funcionalidad se proyecte sin discontinuidades en el tiempo de vida del negocio (Correa, 2018).

La falta de acceso al código fuente profundiza la asimetría técnica que caracteriza a estos contratos. El usuario suele recibir solo una versión ejecutable del software, apta para ser utilizada, pero inhábil para ser modificada o reparada por su cuenta. El control de la estructura interna del sistema queda en manos del proveedor, lo que exige medidas contractuales que impidan que esta concentración de poder tecnológico se

vuelva un riesgo desmedido para el cliente. La doctrina argentina sostuvo que la tutela del usuario en estos escenarios requiere prever mecanismos que permitan mantener la continuidad operativa aun frente al incumplimiento del proveedor o ante eventos que afecten la existencia misma de su empresa (Martínez Barbieri, 2011).

Las obligaciones de mantenimiento y actualización constituyen una pieza indispensable para resguardar el interés económico del usuario. Un software sin soporte pierde rápidamente su adecuación funcional, ya sea por cambios normativos que exigen adaptaciones, por la evolución tecnológica de los sistemas donde opera o por la aparición de vulnerabilidades de seguridad que comprometen datos relevantes. La obligación del proveedor no se satisface con la entrega inicial de la herramienta, sino con su preservación en condiciones que permitan al cliente continuar ejerciendo su actividad sin alteraciones imprevistas. La función primordial del contrato es garantizar que la tecnología siga sirviendo al propósito que motivó la contratación, evitando que el usuario quede expuesto a riesgos no asumidos (Cibils, 2015).

El equilibrio entre la protección intelectual del desarrollador y la protección económica del usuario se logra mediante una técnica contractual cuidadosa. El proveedor conserva sus derechos exclusivos sobre el software, pero el usuario debe contar con remedios efectivos frente a contingencias que podrían paralizar su actividad. Cuando el programa es esencial y no existe sustituto inmediato, la previsión de herramientas como el depósito del código fuente permite conservar la continuidad del negocio sin afectar la propiedad del autor. El contrato se convierte así en un mecanismo de gestión del riesgo tecnológico, asegurando que la dependencia del usuario no derive en una vulnerabilidad irreversible.

En síntesis, el software como objeto de contratación exige contemplar tanto los derechos del creador como la necesidad de que el usuario mantenga en funcionamiento la herramienta que sostiene su desempeño en el mercado. La estabilidad de la prestación se vuelve el parámetro fundamental para evaluar el cumplimiento contractual, y la calidad de la protección jurídica dependerá en gran medida de la claridad y precisión con que se definan los derechos de uso, el alcance del soporte y las garantías mínimas de continuidad del servicio.

Capítulo 5

Depósito del código fuente para asegurar la continuidad operativa

En los contratos informáticos más sensibles, la continuidad del sistema se vuelve un interés central del usuario que no puede quedar librado a la permanencia empresarial del proveedor. Cuando el software contratado sostiene funciones críticas del negocio, el riesgo de que el desarrollador abandone el proyecto o cese su actividad adquiere una dimensión jurídica que exige medidas preventivas. El depósito del código fuente ante un tercero de confianza surgió como respuesta a esta necesidad, permitiendo que el usuario acceda a los elementos técnicos indispensables si el proveedor no puede o no quiere seguir garantizando la operatividad del sistema. Esta figura fue desarrollada doctrinalmente en Argentina como un instrumento eficaz para administrar la dependencia tecnológica dentro de un marco jurídico claro y profesional (Martínez Barbieri, 2011).

El acuerdo de depósito obliga al desarrollador a entregar al depositario una copia completa y actualizada del código fuente, junto con la documentación técnica necesaria para instalarlo y mantenerlo en condiciones operativas. El material permanece resguardado y solo puede ser liberado cuando se cumplan ciertos eventos extraordinarios previstos en el contrato, entre los que se destacan la quiebra del proveedor, la imposibilidad material de continuar la prestación o el incumplimiento grave que afecte directamente la capacidad del usuario de sostener su actividad. La finalidad económica de la herramienta determina el criterio jurídico: no se trata de garantizar un acceso indiscriminado al software, sino de proteger al cliente frente a una contingencia que, de no mediar un remedio adecuado, paralizaría su negocio.

La utilidad real del depósito depende de que el contenido custodiado sea accesible y verificable. Un depósito simbólico carece de valor cuando el usuario, en el momento decisivo, se encuentra con un código incompleto o imposibilitado de uso por falta de instrucciones actualizadas. Por esa razón resulta conveniente establecer en el contrato

procedimientos de actualización periódica, así como controles técnicos que acrediten que el material depositado permite efectivamente poner en funcionamiento el sistema. La verificación puede requerir la participación de un profesional independiente, a fin de asegurar que la custodia no se limite a un acto formal, sino que preserve la funcionalidad práctica del software tal como se utiliza en la operatoria diaria del cliente (Correa, 2018).

El depósito del código fuente no implica la transferencia de los derechos de propiedad intelectual del desarrollador. La liberación del material solo habilita su utilización para sostener la actividad económica del usuario y para ejecutar las modificaciones indispensables que mantengan la herramienta disponible en condiciones normales de trabajo. El alcance del acceso debe quedar claramente definido para evitar que la medida de protección se transforme en una explotación no autorizada del software. La clave radica en armonizar la exclusividad del autor con el derecho del usuario a evitar la paralización de su empresa por causas ajenas a su voluntad. Cuando el contrato delimita correctamente ambas posiciones, la figura se vuelve razonable y atractiva para los dos involucrados (Andreucci, 2016).

En Argentina, su incorporación resulta particularmente útil en contratos de desarrollo a medida, donde el sistema tiene un alto grado de personalización y carece de equivalentes inmediatos en el mercado. El usuario suele construir procesos internos sobre esa solución, lo que refuerza la necesidad de contar con una alternativa técnica viable si la relación contractual sufre una ruptura inesperada. En cambio, en contratos de software estandarizado con múltiples proveedores posibles, la sustitución puede constituir un remedio suficiente, por lo que el depósito del código fuente se vuelve menos necesario. La conveniencia de esta herramienta debe evaluarse entonces según el peso que la solución tecnológica tenga en la continuidad del negocio del cliente y según la existencia de opciones alternativas de reemplazo en plazos compatibles con su actividad.

El depósito del código fuente se integra como un instrumento contractual de prevención y resiliencia, orientado a asegurar que la dependencia tecnológica del usuario no derive en una vulnerabilidad sin retorno. El contrato se transforma así en un mecanismo que no solo distribuye responsabilidades, sino que prepara respuestas concretas frente a los riesgos previsibles que acompañan al uso intensivo de software en la vida económica contemporánea. La protección jurídica se materializa en la capacidad de seguir funcionando aun ante la peor contingencia posible, porque esa es, en definitiva, la meta práctica que motiva la contratación de soluciones informáticas críticas.

Capítulo 6

Hosting y provisión de servicios informáticos en línea

La prestación de servicios informáticos en línea, entre ellos el hosting, se consolidó como un componente estructural de la actividad empresarial. Muchas organizaciones optaron por externalizar la infraestructura necesaria para alojar sus aplicaciones y contenidos digitales, confiando en proveedores que administran servidores, implementan medidas de seguridad y garantizan la disponibilidad permanente del servicio. Este modelo traslada al proveedor una parte central del funcionamiento del negocio del usuario, lo que refuerza la necesidad de precisar contractualmente las obligaciones vinculadas al acceso, el rendimiento y la continuidad del servicio alojado (Cavalli, 2014).

El proveedor de hosting no se limita a poner a disposición un espacio de almacenamiento, sino que asume un rol activo en el mantenimiento de la infraestructura que permite la correcta utilización de la información y de las herramientas que el cliente emplea para su actividad económica. La prestación implica servicios de gestión técnica, comunicaciones seguras, respaldo de datos y resolución de incidentes que puedan afectar la disponibilidad del sistema. La utilidad del contrato se mide, entonces, en función de la estabilidad del servicio prestado y de su capacidad para sostener la operatoria diaria del usuario sin interrupciones imprevistas. Esta dimensión continua convierte al hosting en una obligación en la cual el resultado esperado se proyecta permanentemente en el tiempo de ejecución del contrato.

La doctrina moderna sostiene que la disponibilidad del servicio constituye el núcleo funcional de la prestación. Por este motivo, la fijación de niveles mínimos de operatividad se transformó en una medida fundamental para establecer parámetros claros de cumplimiento. Los acuerdos de nivel de servicio permiten definir estándares verificables y otorgar remedios específicos ante la caída del sistema o la degradación significativa del rendimiento. El proveedor debe adoptar medidas razonables de prevención, monitoreo y recuperación en caso de fallas, mientras que el usuario confía en que la

solución alojada seguirá accesible para su propio tráfico interno o para la interacción con terceros (Izquierdo, 2018).

El hosting plantea además cuestiones vinculadas a la custodia y manejo de información que pertenece al cliente y cuya pérdida o divulgación indebida puede ocasionar perjuicios severos. El proveedor actúa como guardián de los datos y, por ello, debe soportar una carga de diligencia técnica acorde a la sensibilidad del contenido alojado. La protección contra accesos no autorizados, la realización periódica de copias de seguridad y la adopción de medidas de seguridad informática actualizadas se convierten en componentes esenciales de la prestación. El usuario, por su parte, debe respetar las condiciones de uso y asumir la responsabilidad por los contenidos que almacena, pero sin que ello lo despoje del derecho a exigir una protección adecuada de la información que constituye parte de su patrimonio intangible.

La interpretación del contrato debe tener en cuenta el entorno tecnológico en el que se desenvuelve. Una interrupción del servicio no se limita a una pérdida de comodidad técnica, sino que puede afectar la continuidad del negocio del usuario y dañar su reputación comercial. Esta situación exige que el análisis de la responsabilidad del proveedor sea sensible al impacto que el incumplimiento provoca en la operatoria general del cliente, especialmente cuando la prestación es utilizada como medio para el cumplimiento de obligaciones frente a terceros. El hosting funciona como una extensión externa del sistema empresarial del usuario, y esa integración debe reflejarse en la forma en que se evalúa la diligencia requerida al proveedor y las consecuencias que se derivan de una falla en el servicio (Pérez Luño, 2016).

La contratación de servicios informáticos remotos, por lo tanto, requiere un enfoque jurídico que articule la autonomía privada con la protección de la estabilidad operativa del usuario. La libertad contractual es suficiente para ajustar las obligaciones a cada proyecto tecnológico, pero esta libertad debe ejercerse con una comprensión clara de que la disposición del servicio en línea es un presupuesto para la existencia misma del negocio que se apoya en él. El contrato se convierte así en el mecanismo que traduce la confianza técnica del cliente en compromisos concretos del proveedor, permitiendo que la infraestructura externalizada funcione como un soporte seguro, previsible y eficaz para la actividad económica moderna.

Capítulo 7

Seguridad, datos y responsabilidad en entornos digitales

La prestación de servicios informáticos involucra el tratamiento permanente de datos que pertenecen al usuario y que pueden tener relevancia económica, estratégica o personal. La custodia de estos datos se integra a la obligación principal del proveedor, quien debe adoptar medidas adecuadas para preservar su integridad, disponibilidad y confidencialidad durante todo el tiempo de ejecución del contrato. La seguridad informática deja de ser un aspecto accesorio para convertirse en un elemento fundamental de la prestación, ya que una vulneración del sistema puede ocasionar pérdidas significativas y dañar la confianza empresarial tanto frente a clientes como frente a terceros vinculados al negocio del usuario (Cavalli, 2014).

El proveedor asume una posición técnica de guardián de la información, lo que implica actuar con la diligencia que exige el estado de evolución de los sistemas informáticos. La doctrina especializada subrayó que esta responsabilidad técnica no puede interpretarse con los estándares aplicables a bienes materiales, porque el daño en materia informática se produce de modo súbito y con efectos que pueden comprometer toda la estructura operativa del usuario (Molina Quiroga, 2013). La protección contra ataques externos, el control de accesos, el registro de eventos relevantes y la ejecución periódica de copias de respaldo integran un estándar mínimo que debe considerarse al evaluar el cumplimiento contractual. La falta de seguridad adecuada no solo configura un incumplimiento técnico, sino que puede desembocar en responsabilidad por los perjuicios que se deriven de incidentes evitables mediante medidas razonables. La evaluación jurídica de la diligencia se realiza atendiendo a los riesgos inherentes a la prestación y a la necesidad objetiva de prevenirlos mediante controles preventivos técnicamente aceptados (Pérez Luño, 2016).

La confidencialidad constituye otro eje de protección. El usuario deposita información en la infraestructura del proveedor confiando en que no será utilizada para fines

distintos a los estrictamente necesarios para la prestación del servicio. Las cláusulas de confidencialidad deben prever obligaciones claras de resguardo y sanciones proporcionadas frente a accesos indebidos o filtraciones ocasionadas por una actuación negligente del proveedor o de su personal. La protección de secretos comerciales y datos sensibles se vuelve indispensable para mantener la competitividad del usuario en el mercado y evitar que la externalización de infraestructura tecnológica se transforme en una amenaza para su patrimonio inmaterial.

La integridad y disponibilidad de los datos también inciden directamente en la continuidad del negocio del usuario. Un incidente que afecte la información esencial para la gestión del sistema puede tener el mismo impacto que una caída completa del servicio. La responsabilidad del proveedor se extiende a las pérdidas generadas por deficiencias en las medidas de prevención y en la capacidad de recuperación frente a una falla. La prestación debe contemplar planes de contingencia que permitan restablecer la operatividad en plazos razonables, asegurando que el usuario no sufra consecuencias desproporcionadas frente a contingencias previsibles y gestionables mediante una adecuada planificación técnica.

El régimen de responsabilidad aplicable se basa en los principios tradicionales del derecho argentino. Sin embargo, la posición de dependencia técnica del usuario exige interpretar estos principios con un enfoque acorde a la naturaleza de la prestación. La omisión de soporte, actualizaciones o medidas de seguridad puede configurar un incumplimiento grave cuando afecta la función económica principal del contrato y expone al cliente a la paralización de su negocio (Molina Quiroga, 2013). La prueba del daño puede resultar compleja cuando se trata de información digital, pero la relación causal se identifica claramente cuando el incidente provoca la pérdida de datos o interrumpe una actividad cuya preservación constituía parte de la finalidad económica del acuerdo (Lorenzetti, 2015).

La externalización de servicios tecnológicos permite reducir costos y acceder a infraestructura profesionalizada, pero exige asegurar que la estructura jurídica acompañe la sensibilidad del riesgo que asume el usuario al trasladar información y procesos esenciales fuera de su ámbito de control directo. La seguridad, la custodia de datos y la responsabilidad que se deriva de su manejo forman parte de las condiciones que hacen viable la contratación informática como herramienta de crecimiento y competitividad sin comprometer la estabilidad operativa del negocio.

Capítulo 8

Criterios contractuales para la resiliencia tecnológica

El objetivo central de los contratos informáticos es sostener la continuidad del negocio del usuario en un entorno donde la tecnología se volvió indispensable para la actividad económica. Esta finalidad exige que el acuerdo contemple mecanismos específicos que permitan gestionar los riesgos que surgen de la dependencia técnica existente entre las partes. La resiliencia tecnológica del contrato se alcanza mediante una combinación de previsiones orientadas a garantizar la operatividad del sistema, distribuir adecuadamente los riesgos de interrupción y asegurar respuestas eficientes cuando se materializa una contingencia.

Para que la solución informática cumpla efectivamente su propósito, el contrato debe definir con claridad la funcionalidad comprometida, el alcance del soporte técnico y los parámetros mínimos de disponibilidad del servicio. La descripción de estas obligaciones no puede limitarse a enunciados genéricos, sino que requiere especificaciones que faciliten la verificación del cumplimiento y permitan actuar frente a desvíos que afecten el rendimiento operativo del sistema. La tutela de la continuidad se refuerza con la inclusión de tiempos máximos de respuesta ante incidentes, procedimientos de comunicación y responsabilidad directa frente a la afectación del servicio que derive de la negligencia del proveedor.

La adopción de soluciones preventivas resulta indispensable para administrar la exposición del usuario frente a la eventual indisponibilidad del proveedor. El depósito del código fuente, la disponibilidad de documentación técnica actualizada y la posibilidad de recurrir a terceros para realizar tareas de mantenimiento se presentan como medidas que reducen la dependencia absoluta del desarrollador y protegen al cliente ante eventos extraordinarios. Estas previsiones reflejan una comprensión madura del riesgo tecnológico y permiten asegurar que la continuidad del negocio no quede comprometida por causas ajenas al usuario. La estructura obligacional en estos contratos

debe incorporar mecanismos que resguarden el valor económico de la relación, ya que la utilidad del servicio depende de que la herramienta permanezca plenamente operativa y disponible durante su ciclo de vida funcional (Molina Quiroga, 2001).

El resguardo de la información también debe integrarse con la finalidad de resiliencia operativa. El proveedor debe asumir un compromiso efectivo de seguridad técnica que abarque la protección contra accesos no autorizados, la prevención de pérdidas de datos y la ejecución de copias de seguridad en condiciones adecuadas. El usuario deposita su confianza en la infraestructura del proveedor y esa confianza debe traducirse en obligaciones precisas que preserven los datos como parte esencial del soporte de su actividad económica. La indisponibilidad de la información puede generar un perjuicio igual o mayor que una caída completa del servicio, por lo que la responsabilidad del proveedor sobre su custodia resulta insoslayable.

Los contratos informáticos deben estructurarse, en definitiva, como mecanismos que combinan cooperación técnica y protección jurídica. La asignación de riesgos no puede desentenderse del impacto que una contingencia operativa puede producir en la organización del cliente. La doctrina especializada advirtió que la falta de diligencia en la continuidad técnica puede constituir un incumplimiento grave, en tanto afecta el núcleo económico del acuerdo y expone al usuario a pérdidas que no está obligado a soportar (Molina Quiroga, 2013). La previsión contractual adecuada fortalece la estabilidad del negocio y promueve un entorno de confianza donde el proveedor asume conscientemente el papel central que desempeña en la estructura empresarial del usuario. Cuando los remedios contractuales permiten anticipar soluciones frente a eventos que podrían paralizar el sistema, el contrato cumple su función como herramienta eficaz de protección económica en un escenario donde la tecnología es parte esencial del patrimonio operativo de las empresas argentinas.

Capítulo 9

Conclusiones

La contratación informática en el derecho argentino se consolidó como una herramienta indispensable para la protección de la continuidad operativa de los negocios que dependen de sistemas tecnológicos. La transformación digital de las empresas no solo introdujo nuevas modalidades contractuales, sino que también modificó la forma en que se evalúan los riesgos y las responsabilidades en la interacción entre usuarios y proveedores de tecnología. La función económica de estos contratos se centra en garantizar el acceso permanente a recursos técnicos que resultan esenciales para la existencia misma de la actividad comercial.

El análisis desarrollado permitió identificar que la dependencia tecnológica genera una posición de vulnerabilidad del usuario que se debe atender desde la estructura jurídica del contrato. La tutela comienza en la etapa precontractual, cuando el proveedor debe brindar información suficiente y adecuada para que el cliente pueda adoptar decisiones conscientes sobre la solución que incorpora a su organización. Continúa en la fase de ejecución, donde el valor del contrato se mantiene solo si la operatividad del sistema permanece estable, segura y actualizada.

El equilibrio contractual exige reconocer los derechos del desarrollador sobre el software y los servicios que presta, sin que esta protección se traduzca en un riesgo desmedido para el usuario. Medidas como el mantenimiento continuo, la fijación de niveles mínimos de disponibilidad del servicio y la protección de datos alojados en infraestructura externa se revelan como componentes esenciales del contenido obligacional. A ello se suma la conveniencia de incorporar herramientas preventivas, como el depósito del código fuente en casos de software crítico, que permiten enfrentar contingencias graves sin poner en riesgo la continuidad del negocio.

El derecho argentino, sin necesidad de crear categorías autónomas, ya ofrece principios y remedios suficientes para regular la contratación informática. Sin embargo, la correcta aplicación de estos instrumentos exige una técnica contractual afinada, capaz de traducir con precisión la realidad tecnológica en obligaciones jurídicas verificables.

La cooperación entre proveedor y usuario debe estructurarse mediante cláusulas claras, orientadas a asegurar que la prestación tecnológica cumpla su finalidad práctica durante todo el ciclo de vida del negocio que se apoya en ella.

La protección jurídica en este ámbito se mide en términos de estabilidad, seguridad y resiliencia. Un contrato bien diseñado permite que la innovación tecnológica no se convierta en una fuente de vulnerabilidad, sino en un motor de desarrollo económico sostenido. La contratación informática tiene así la responsabilidad de garantizar que el progreso digital llegue acompañado de instrumentos jurídicos que preserven la continuidad de las actividades empresariales y el equilibrio legítimo de intereses entre quienes producen la tecnología y quienes la necesitan para existir en el mercado.

Bibliografía

Altmark, D. R. (1987). La etapa precontractual en los contratos informáticos. En D. R. Altmark (Dir.) y R. A. Bielsa (Coord.), *Informática y derecho: Aportes de doctrina internacional* (Vol. 1). Depalma.

Andreucci, F. (2016). *Software y bases de datos en el derecho de autor argentino*. Dirección Nacional del Derecho de Autor (DNDA).

Cavalli, J. (2014). Servicios en la nube y obligaciones del proveedor. *Revista de Derecho y Tecnología, 3*, 91–112.

Cibils, A. (2015). *Contratos electrónicos y protección al consumidor*. La Ley.

Correa, C. M. (2018). Propiedad intelectual y tecnologías de la información. *Revista Jurídica, 12*, 33–54.

Izquierdo, M. (2018). Infraestructura virtual y traspaso de riesgos en contratos informáticos. *Revista Jurídica, 14*, 55–70.

Lorenzetti, R. L. (2015). *Código Civil y Comercial de la Nación comentado* (Toms. I–V). Rubinzal-Culzoni.

Martínez Barbieri, M. S. (2011). El depósito de código fuente (escrow) y la continuidad del negocio. *Revista de Derecho Informático, 53*, 1–15.

Molina Quiroga, E. (2001). *Contratos informáticos*. Astrea.

Molina Quiroga, E. (2013). Responsabilidad contractual en contratos informáticos. En P. Patrón Bedoya y F. Bueno de Mata (Coords.), *Nuevas tecnologías y justicia 2.0: Estudios en homenaje al Prof. Dr. D. Valentín Carrascosa López* (Vol. 2, pp. 35–60). Parlamento de Extremadura.

Pérez Luño, A. E. (2016). *Derechos humanos y revolución digital*. Tirant lo Blanch.